



PROJETO DE LEI Nº , DE 2026

(Do Sr. Dep. Cabo Gilberto Silva)

Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tipificar o crime de manipulação fraudulenta de sistema de inteligência artificial e dá outras providências.

O Congresso Nacional decreta:

Art. 1º - O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), passa a vigorar acrescido do seguinte art. 154-C:

“Manipulação fraudulenta de sistema de inteligência artificial

Art. 154-C. Inserir, ocultar, dissimular, transmitir ou utilizar comando, instrução, código, metadado ou conteúdo de caráter fraudulento, oculto ou não autorizado, capaz de comprometer a integridade funcional de sistema de inteligência artificial empregado em processo de tomada de decisão, de análise, de triagem, de classificação, de autenticação ou de recomendação, com o fim específico de obter vantagem ilícita, causar dano a terceiro, acessar indevidamente dado pessoal, dado pessoal sensível, dado sigiloso protegido por lei ou informação submetida a dever legal de confidencialidade, ou induzir decisão automatizada ou assistida por inteligência artificial em prejuízo de terceiro:

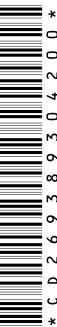
Pena - reclusão, de 1 (um) a 2 (dois) anos, e multa, se o fato não constitui crime mais grave.

§ 1º A pena é de reclusão, de 2 (dois) a 4 (quatro) anos, e multa, se

da conduta resultar:

I - obtenção, alteração, destruição, ocultação ou divulgação indevida de dado pessoal, dado pessoal sensível, dado sigiloso protegido por lei ou informação submetida a dever legal de

confidencialidade;



II - prejuízo econômico superior a 40 (quarenta) salários mínimos, considerado o benefício obtido pelo agente ou o dano causado à vítima;

III - interferência em processo judicial, administrativo, legislativo, regulatório, eleitoral, licitatório ou seletivo, com potencial de alterar o seu resultado, classificação, decisão ou ato;

IV - comprometimento da continuidade, da segurança ou da integridade de serviço público essencial ou de infraestrutura crítica definida em lei ou regulamento; ou

V - indução de decisão automatizada ou assistida por inteligência artificial que prejudique terceiro.

§ 2º A pena é aumentada de um terço se o crime for praticado:

I - contra criança, adolescente, pessoa idosa ou pessoa que, por enfermidade, deficiência ou outra condição juridicamente reconhecida, tenha reduzida capacidade de compreender ou de resistir à conduta;

II - contra órgão ou entidade da Administração Pública direta ou indireta, Poder Legislativo, Poder Judiciário, Ministério Público, Defensoria Pública, Tribunal de Contas, agência reguladora, serviço público essencial ou infraestrutura crítica definida em lei ou regulamento;

III - mediante uso de identidade falsa, documento falso, automação em larga escala, ocultação deliberada de autoria ou emprego de mecanismo destinado a dificultar a identificação do agente;

IV - por agente que se aproveite de posição profissional, funcional, contratual ou técnica que lhe confira acesso, conhecimento ou privilégio operacional relevante para facilitar a prática delitiva.

§ 3º Não constitui crime a realização de teste, auditoria, pesquisa de segurança, ensino, demonstração técnica, teste adversarial autorizado, validação, desenvolvimento ou correção de vulnerabilidade, desde que ausentes a finalidade fraudulenta, a obtenção de vantagem ilícita, o dano deliberado a terceiro e o acesso indevido a dado pessoal, dado pessoal sensível, dado sigiloso protegido por lei ou informação submetida a dever legal de confidencialidade.

§ 4º Para os fins deste artigo, considera-se sistema de inteligência artificial o sistema baseado em máquina que, com





graus diferentes de autonomia e para objetivos explícitos ou implícitos, infere, a partir de um conjunto de dados ou informações que recebe, como gerar resultados, em especial previsão, conteúdo, recomendação ou decisão que possam influenciar o ambiente virtual, físico ou real.” (NR)

Art. 2º - O art. 154-B do Decreto-Lei nº 2.848, de 7 de dezembro de 1940, passa a vigorar com a seguinte redação:

“Art. 154-B. Nos crimes definidos nos arts. 154-A e 154-C, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios, contra empresas concessionárias de serviços públicos, serviço público essencial, infraestrutura crítica definida em lei ou regulamento ou pessoa referida no inciso I do § 2º do art. 154-C, ou se houver obtenção, divulgação, extração ou comprometimento de dado pessoal sensível, dado sigiloso protegido por lei ou informação submetida a dever legal de confidencialidade.” (NR)

Art. 3º - Esta Lei entra em vigor na data de sua publicação oficial.

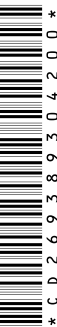
JUSTIFICATIVA

O acelerado desenvolvimento e a crescente utilização de sistemas de inteligência artificial em atividades públicas e privadas têm transformado profundamente a forma como decisões são tomadas, informações são processadas e serviços essenciais são prestados. Atualmente, sistemas de inteligência artificial são empregados em procedimentos administrativos, processos judiciais, instituições financeiras, serviços de saúde, infraestrutura crítica, plataformas digitais, autenticação de identidade, análise de crédito, prevenção a fraudes, seleção de candidatos, licitações e inúmeras outras atividades cuja confiabilidade possui impacto direto sobre direitos individuais e interesses coletivos.

Paralelamente aos benefícios proporcionados por essa tecnologia, surgem novas modalidades de fraude e de ataques cibernéticos voltadas especificamente à manipulação do funcionamento

Para verificar a assinatura, acesse <https://infoleg-autenticidade-assinatura.camara.leg.br/CD269389304200>

Assinado eletronicamente pelo(a) Dep. Cabo Gilberto Silva



desses sistemas. Técnicas como a inserção de comandos ocultos (prompt injection), a contaminação de dados (data poisoning), a manipulação de modelos (model poisoning) e outras formas de adulteração de entradas e instruções podem comprometer a integridade dos resultados produzidos pela inteligência artificial, ocasionando prejuízos patrimoniais, violação da privacidade, exposição de informações protegidas por sigilo legal e decisões automatizadas injustas ou fraudulentas.

Embora o ordenamento jurídico brasileiro possua instrumentos destinados à repressão de crimes informáticos, especialmente os arts. 154-A e 154-B do Código Penal, tais dispositivos foram concebidos para tutelar principalmente a invasão de dispositivos informáticos e não alcançam, de forma específica, a manipulação fraudulenta de sistemas de inteligência artificial sem que necessariamente haja invasão do equipamento ou acesso indevido ao dispositivo.

A ausência de tipificação específica cria relevante lacuna normativa diante da rápida evolução tecnológica, comprometendo a efetividade da tutela penal em situações nas quais agentes manipulam o comportamento de sistemas inteligentes para obtenção de vantagem ilícita, acesso indevido a informações protegidas ou indução de decisões automatizadas em prejuízo de terceiros.

A Constituição Federal impõe ao Estado o dever de assegurar a proteção dos direitos fundamentais, da segurança jurídica e da ordem pública. Nos termos do art. 5º, caput, são assegurados a inviolabilidade da vida, da liberdade, da igualdade, da segurança e da propriedade. O inciso X protege a intimidade, a vida privada, a honra e a imagem das pessoas, enquanto o inciso XII assegura a inviolabilidade do sigilo das comunicações e dos dados, ressalvadas as hipóteses legais. Tais garantias constitucionais exigem mecanismos jurídicos capazes de responder às novas formas de criminalidade decorrentes da transformação digital.

Igualmente, o art. 37 da Constituição estabelece que a Administração Pública deve observar os princípios da legalidade, impessoalidade, moralidade, publicidade e eficiência. A crescente utilização de sistemas de inteligência artificial na gestão pública torna indispensável a existência de instrumentos legais destinados a preservar sua integridade, confiabilidade e funcionamento regular, evitando que manipulações fraudulentas comprometam decisões administrativas ou afetem a adequada prestação dos serviços públicos.

O projeto também encontra fundamento na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), que reconhece como fundamentos da disciplina da proteção de dados o respeito à privacidade, à autodeterminação informativa, à inviolabilidade da intimidade e ao livre desenvolvimento da personalidade da pessoa natural. Os princípios da segurança, da prevenção e da responsabilização, previstos no art. 6º da referida lei, reforçam a necessidade de proteção jurídica contra condutas destinadas à obtenção ou exposição indevida de dados pessoais por meio da manipulação de sistemas de inteligência artificial.

Para verificar a assinatura, acesse <https://infoleg-autenticidade-assinatura.camara.leg.br/C269389304200>

Assinado eletronicamente pelo(a) Dep. Cabo Gilberto Silva





A proposição também se harmoniza com o Marco Civil da Internet (Lei nº 12.965, de 23 de abril de 2014), que estabelece como princípios do uso da internet no Brasil a proteção da privacidade, dos dados pessoais, da estabilidade, da segurança e da funcionalidade da rede, impondo ao Poder Público o dever de promover ambiente digital seguro e confiável.

No plano internacional, observa-se crescente preocupação com a segurança dos sistemas de inteligência artificial. Organismos internacionais, como a Organização para a Cooperação e Desenvolvimento Econômico (OCDE), bem como o Regulamento Europeu de Inteligência Artificial (AI Act) da União Europeia, reconhecem a necessidade de adoção de mecanismos destinados a assegurar a confiabilidade, a segurança e a integridade desses sistemas, especialmente quando empregados em atividades capazes de produzir impactos relevantes sobre direitos fundamentais.

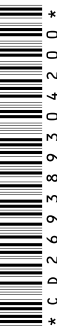
A proposta observa rigorosamente os princípios da legalidade, da taxatividade e da intervenção mínima do Direito Penal. O tipo penal exige dolo específico, consistente na finalidade de obtenção de vantagem ilícita, causação de dano, acesso indevido a informações protegidas ou indução fraudulenta de decisões automatizadas, afastando a criminalização de condutas culposas ou de meras falhas técnicas.

Além disso, o projeto prevê expressamente hipótese de exclusão da tipicidade para atividades legítimas de pesquisa científica, auditoria de segurança, testes autorizados, desenvolvimento tecnológico e correção de vulnerabilidades, preservando a atuação de pesquisadores, instituições acadêmicas, profissionais de segurança da informação e programas de divulgação responsável de vulnerabilidades.

As causas de aumento de pena e as formas qualificadas propostas observam critérios objetivos de maior reprovabilidade da conduta, especialmente quando a manipulação atingir crianças, adolescentes, idosos, pessoas em situação de vulnerabilidade, órgãos públicos, serviços públicos essenciais, infraestruturas críticas ou resultar na obtenção indevida de dados protegidos ou em prejuízo econômico de elevada expressão.

Dessa forma, a presente proposição busca suprir importante lacuna do ordenamento jurídico brasileiro, conferindo proteção penal adequada à integridade dos sistemas de inteligência artificial, sem comprometer a inovação tecnológica, a pesquisa científica ou o desenvolvimento da economia digital, fortalecendo a segurança jurídica, a confiança nas novas tecnologias e a proteção dos direitos fundamentais.

Ante o exposto, considerando a relevância da matéria para a proteção da sociedade, da Administração Pública, da economia digital e dos direitos fundamentais assegurados pela Constituição da República, contamos com o apoio dos ilustres Parlamentares para a aprovação da



presente proposição.

Sala das sessões, em de
2026.

DEPUTADO CABO GILBERTO SILVA
(PL/PB)

Apresentação: 14/07/2026 17:17:57.233 - Mesa

PL n.3695/2026



Para verificar a assinatura, acesse <https://infoleg-autenticidade-assinatura.camara.leg.br/CD269389304200>
Assinado eletronicamente pelo(a) Dep. Cabo Gilberto Silva

